Variation Agreement

Variation Reference: GDPR

Proposed by: NHS England

Date of Proposal: 21 August 2018

Date of Variation Agreement: 21 August 2018

Capitalised words and phrases in this Variation Agreement have the meanings given to them in the Agreement referred to above.

1. The Parties have agreed the [National] Variation summarised below:

10.2 replace 'govern' with 'describe'
10.3 add 'Schedule 4'
Schedule 1: Definitions and interpretation:

- Replace references to the Data Protection Act (DPA) with GDPR (the General Data Protection Regulation).
- Replace reference to the DPA, the EU Data Protection Directive 95/46/EC with reference to GDPR, the Data Protection Act 2018
- Replace 'Sensitive Personal Data' with 'Special Category Personal Data'

Schedule 4: Further Information Sharing Provisions

- 4.2
- 6.2 Replace 'Sensitive Personal Data' with 'Special Category Personal Data'
- 7.1 Replace DPA with GDPR
- 7.1.2 Amend to: 'amendment of respective privacy notices and policies to reflect the processing of data carried out further to this agreement, including covering the requirements of articles 13 and 14 GDPR and providing these (or making them available to) Data Subjects;'
- 7.2 Amend to: 'Each Party shall procure that its notification to the Information Commissioner's Office and record of processing maintained for the purposes of Article 30 GDPR reflects the flows of information under this Agreement'.
- 8.1, 8.3, 9.2, 9.3, 9.4.2, 9.4.3, 9.5.2: Replace 'Sensitive Personal Data' with 'Special Category Personal Data'
- 8.2 Replace 'DPA' with 'Data Protection Act 2018'
- 9.3.2 Amend to: 'in respect of the Relevant Information it shall promptly (and within 48 hours) notify the other Party. The Parties shall fully cooperate with one another to remedy the issue as soon as reasonably practicable, and in making information about the incident available to the Information Commissioner and Data Subjects where required by Information Law.'
- 9.4.1 Amend to: 'process the Personal Data (including Special Category Personal Data) only in accordance with the terms of this Agreement and otherwise (to the extent that it acts as a Data Processor for the purposes of Article 27-28 GDPR) only in accordance with written instructions from the originating Data Controller in respect of its Relevant Information;
- 9.4.4 Amend to: 'process the Personal Data in accordance with the requirements of Information Law and in particular the principles set out in Article 5(1) and accountability requirements set out in Article 5(2) GDPR.'
- 9.5 – 9.9 Amend to:
  9.5 Each Party shall act generally in accordance with Information Law

requirements, and in particular shall implement, maintain and keep under review appropriate technical and organisational measures to ensure and to be able to demonstrate that the processing of Personal Data is undertaken in accordance with Information Law, and in particular to protect the Personal Data (and Special Category Personal Data) against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall:

9.5.1 Take account of the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of Data Subjects; and

9.5.2 Be appropriate to the harm which might result from any unauthorised or unlawful processing, accidental loss, destruction or damage to the Personal Data (and Special Category Personal Data) and having regard to the nature of the Personal Data (and Special Category Personal Data) which is to be protected.

9.6 In particular, each Party shall:

9.6.1 ensure that only Personnel authorised under this Agreement have access to the Personal Data (and Special Category Personal Data);

9.6.2 ensure that the Relevant Information is kept secure and in an encrypted form, and shall use all reasonable security practices and systems applicable to the use of the Relevant Information to prevent and to take prompt and proper remedial action against, unauthorised access, copying, modification, storage, reproduction, display or distribution, of the Relevant Information;

9.6.3 obtain prior written consent from the originating Party in order to transfer the Relevant Information to any third party;

9.6.4 permit the other Party or their representatives (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit the data processing activities carried out further to this Agreement (and/or those of its agents, successors or assigns) and comply with all reasonable requests or directions to enable each Party to verify and/or procure that the other is in full compliance with its obligations under this Agreement; and

9.6.5 if requested, provide a written description of the technical and organisational methods and security measures employed in processing Personal Data.

9.7 Specific requirements as to information security set out in the Personal Data Agreement(s).

9.8 Each Party shall use best endeavours to achieve and adhere to the requirements of the NHS Information Governance Toolkit, particularly in relation to Confidentiality and Data Protection Assurance, Information Security Assurance and Clinical Information Assurance.

9.9 The Parties' Single Points of Contact (**"SPoC"**) set out in paragraph 14 *(Governance: Single Points of Contact)* below will be the persons who, in the first instance, will have oversight of third party security measures.

- 10.4 Add 'and held'
- 11.1 Add 'and to comply with the principles set out in Article 5(1)(c) and (d) GDPR.'
- 12.4 Replace 'the fifth Data Protection Principle' with 'requirements of 5 (1) (e) GDPR'
- 12.1 Add 'as well as any other purported exercise of a Data Subject's rights under Information Law or complaint to or investigation undertaken by the Information Commissioner.'
- Template Personal Data Agreement – changes to formatting, replace DPA Schedule 2 condition/s with 'GDPR Article 6 legitimising conditions' and replace 'DPA Schedule 3 condition/s' with GDPR Article 9 legitimising conditions'

2. The National Variation is reflected in the attached Schedule and the Parties agree that the Agreement is varied accordingly.

3. The Variation takes effect on 21 August 2018

IN WITNESS OF WHICH the Parties have signed this Variation Agreement on the date(s) shown below

Signed by **NHS England**

Paul Baumann for and on behalf of NHS England

Signed by **[ ] Clinical Commissioning Group**

[ ] (for and on behalf of [ ])